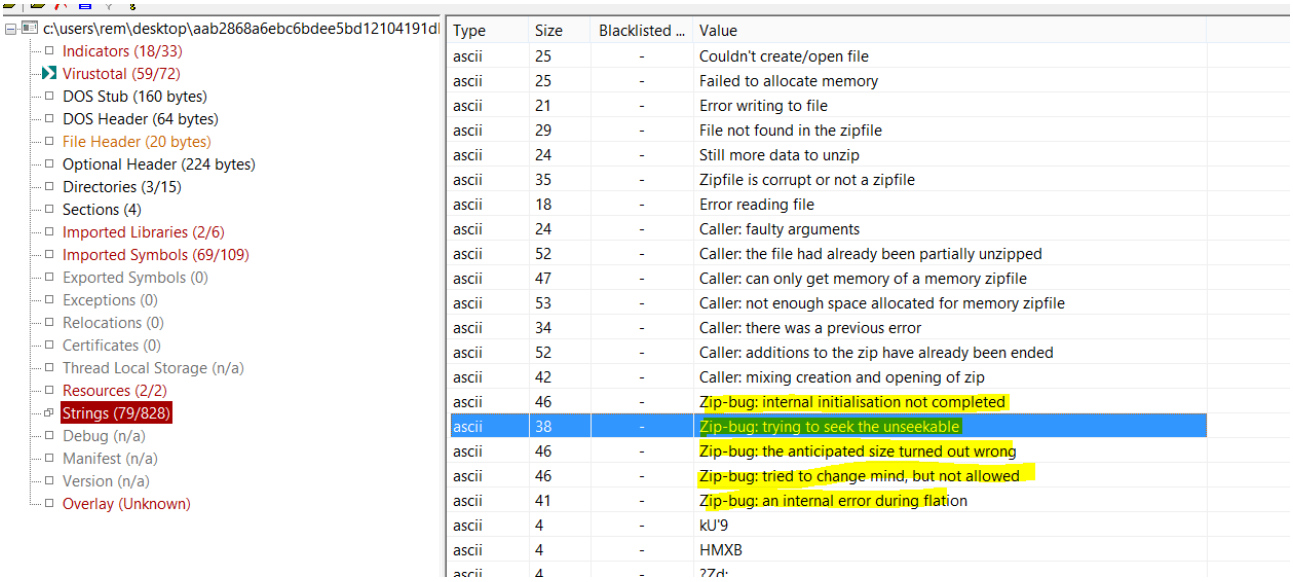
PebbleDash - Lazarus / HiddenCobra RAT

By malwarenailed

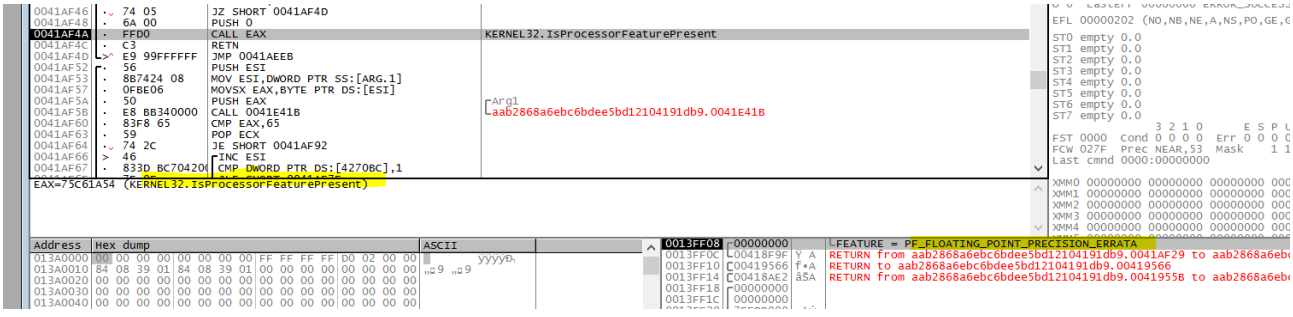
Published: 2020-06-01 · Archived: 2026-04-05 13:27:57 UTC

Hi folks. I was analyzing the PebbleDash malware used by Lazarus APT group. While analyzing the original sample (Md5: d2de01858417fa3b580b3a95857847d5), I was able to find out the C2 server and the port, where it intends to communicate to. I also found an interesting technique it uses to identify the OS version of the victim machine.

During static analysis, I observed interesting strings were starting with "Zip-bug", as can be seen below. Using yara rules I was able to discover some other samples uploaded to HA (Hybrid Analysis) with the same strings embedded. These samples seemed to be not related to d2de01858417fa3b580b3a95857847d5. However, they communicated to South Korea and China.

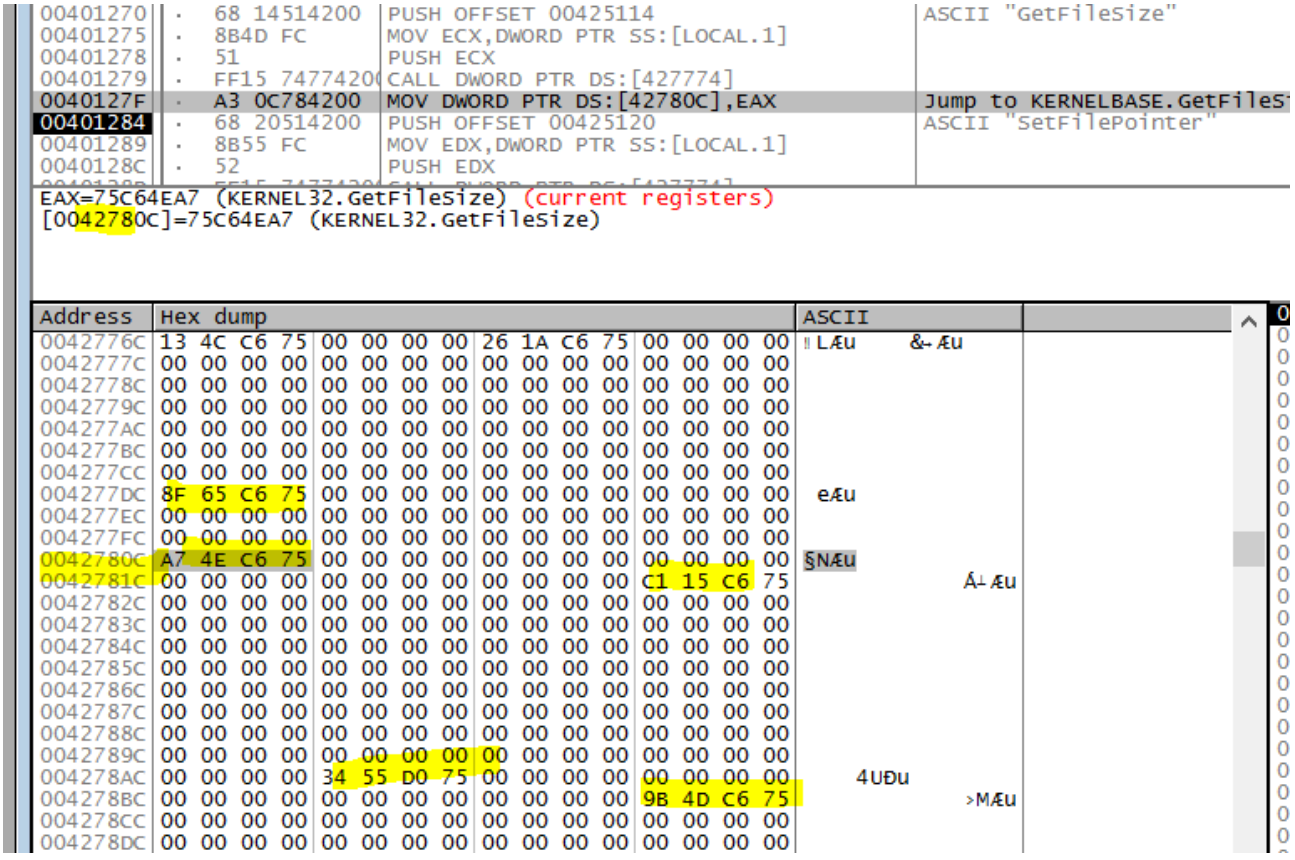


While performing dynamic anlaysis, I observed that the sample uses the API call IsProcessorFeaturePresent to determine the version of the victim OS. The PF_FLOATING_POINT_PRECISION_ERRATA feature is explicitly set to FALSE in x86 version 6.1 and higher.

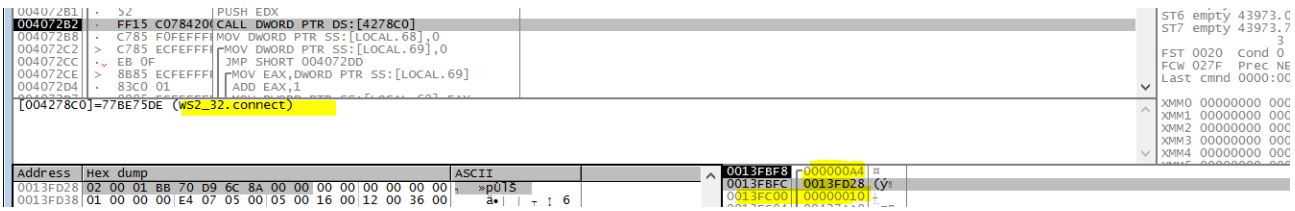


The sample loads several libraries dynamically during run time. This also included wsock32.dll. Malware usually does this as an anti-analysis technique (anti static analysis)

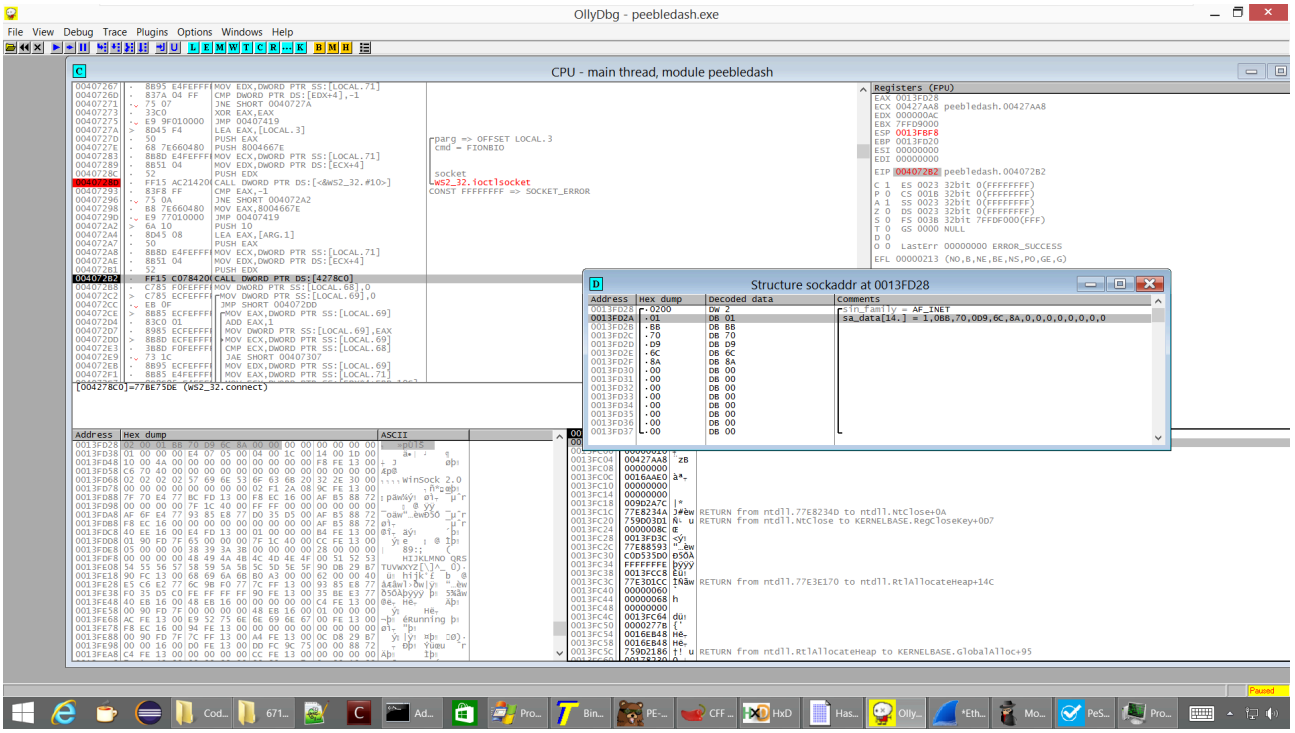
After loading the libraries the malware saves the memory offset of the API functions it intends to use as can be seen below.



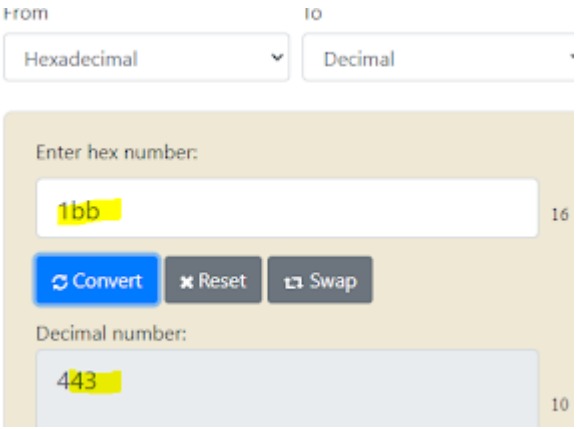
It then tries to open a socket connection by calling the connect function.



I decoded the "sockaddr" structure which is passed on to the connect function.



The first two bytes in the structure represents the destination port and we can see that it is 443 in this case.



The rest of the four bytes are: 0x70 0xd9 0x6C 0x8A, which translates to 112.217.108.138 (hex to decimal). This is the C2 ip address where PebbleDash communicates to. This IOC also be seen in the US-CERT advisroy.

terminate processes, and perform target system enumeration.

For a downloadable copy of IOCs, see MAR-10288834-3.v1.stix.

Submitted Files (1)

aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6 (D2DE01858417FA3B580B3A958

IPs (1)

112.217.108.138

Findings

aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6

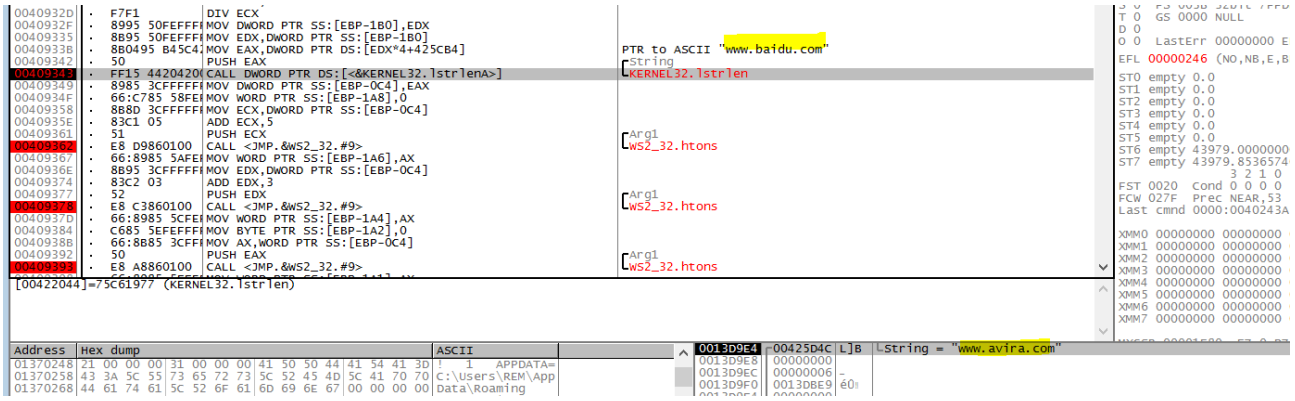
Tags

rootkit trojan

Details

Name	D2DE01858417FA3B580B3A95857847D5
Size	167937 bytes

PebbleDash inserts fake "server name" in the TLS packet. We can see below some:



Source: https://malwarenailed.blogspot.com/2020/06/peebledash-lazarus-hiddencobra-rat.html